APPENDIX OF CLAIMS

1(Amended). A method for storing and retrieving a number of PIN codes for protected access devices, comprising the following steps for storing the PIN codes:

entering and at least briefly storing an access code,

entering and storing at least one PIN code of a protected-access device,

entering and storing at least one unique feature of at least one protected-access device,

producing a link between one of the stored PIN codes and the stored unique feature of that device with protected access through the relevant PIN code;

and the following steps for retrieving a specific stored PIN code:

entering the access code,

entering the unique feature of the protected-access device associated with the PIN code to be retrieved,

testing whether the access code is permissible,

testing whether the entered unique feature matches one of the stored unique features, and

if both tests turn out positive, outputting the stored PIN code linked with the unique feature.

2(Amended). The method according to claim 1, including storing the stored access code permanently and testing the permissibility of the entered access code with reference to a comparison with the permanently stored access code.

3(Amended). The method according to either of claim 1, including storing the access code and/or unique features and/or PIN codes in encoded form.

4(Amended). The method according to claim 3, including using the access code as a key for encoded storage.

5(Amended). The method according to claim 4, including storing the access code only briefly and deleting the access code after encoding has taken place.

6(Amended). The method according to claim 4, including effecting the linking between the unique feature of a protected-access device and the associated PIN code by encoding the PIN code, and wherein the unique feature forms the key.

7(Amended). The method according to claim 1, wherein the access code and/or unique features and/or PIN codes are stored in externally inaccessible memory areas.

8(Amended). The method according to claim 1, wherein the particular serial number of the protected-access device is used as the unique feature.

9(Amended). The method according to claim 1, wherein a characteristic physical property of the protected-access device is used as the unique feature.

10(Amended). The method according to claim 1, wherein the unique feature is automatically determined and entered.

11(Amended). The method according to claim 1, wherein the output of the PIN code is made available only for a limited time period.

12(Amended). The method according to claim 1, wherein the protected-access devices comprise smart cards and/or magnetic stripe cards.

13(Amended). The method according to claim 1, wherein a wrong PIN code not stored is outputted if one of the two tests turns out negative.

14(Amended). An apparatus for storing and retrieving a number of PIN codes for protected-access devices, comprising

a keyboard for entering the PIN codes and an access code,

a device for receiving unique features of the protected-access devices,

at least one memory for at least briefly storing the access code, storing the PIN codes and storing the unique features,

a device for testing an entered access code as to its permissibility and comparing an entered unique feature with stored unique features, and

a display for indicating retrieved PIN codes.

15(Amended). The apparatus according to claim 14, wherein the apparatus is a pocket card reader.

16(Amended). The apparatus according to claim 13 including a device for encoding the PIN codes and/or unique features and/or access code.

17(Amended). The apparatus according to claim 14, including externally inaccessible memory areas for storing the PIN codes and/or unique features and/or access code.

18(Amended). The apparatus according to claim 14, wherein the keyboard constitutes the device for receiving the unique features.

19(Amended). The apparatus according to claim 14, wherein the device for receiving the unique features includes a device for automatically determining the unique features of the access-protected devices.

S:\Producer\jek\KOLBECK - KOLB3001\appendix of claims.wpd

International Application No. PCT/EP00/04781
Attorney Docket No.: KOLB3001/JEK

APPENDIX OF MARKED-UP VERSION OF CLAIMS

1(Amended). A method for storing and retrieving a number of PIN codes for protected access devices, comprising the following steps for storing the PIN codes:[, namely]

[-] entering and at least briefly storing an access code,

[-] entering and storing at least one PIN code of a protected-access device,

[-] entering and storing at least one unique feature of at least one protected-access device,

[-] producing a link between one of the stored PIN codes and the stored unique feature of that device with protected access through the relevant PIN code; [and]

and the following steps for retrieving a [certain] specific stored PIN code:[, namely]

[-] entering the access code,

[-] entering the unique feature of the protected-access device associated with the PIN code to be retrieved,

[-] testing whether the access code is permissible,

[-] testing whether the entered unique feature matches one of the stored unique features, and

[-] if both tests turn out positive, outputting the stored PIN code linked with the unique feature.

2(Amended). [A] The method according to claim 1, [characterized in that] including storing the stored access code [is stored] permanently and testing the permissibility of the entered access code [is tested] with reference to a comparison with the permanently stored access code.

3(Amended). [A] The method according to either of [claims] claim 1 [and 2], [characterized in that] including storing the access code and/or unique features and/or PIN codes [are stored] in encoded form.

4(Amended). [A] The method according to claim 3, [characterized in that] including using the access code [is used] as a key for encoded storage.

5(Amended). [A] The method according to claim 4, [characterized in that] including storing the access code [is stored] only briefly and [deleted] deleting the access code after encoding has taken place.

6(Amended). [A] The method according to [any of claims 1 to 5, characterized in that] claim 4, including effecting the linking between the unique feature of a protected-access device and the associated PIN code [is effected] by encoding the PIN code, and wherein the unique feature [forming] forms the key.

7(Amended). [A] The method according to [any of claims 1 to 6, characterized in that] claim 1, wherein the access code and/or unique features and/or PIN codes are stored in externally inaccessible memory areas.

8(Amended). [A] The method according to [any of claims 1 to 7, characterized in that] claim 1, wherein the particular serial number of the protected-access device is used as the unique feature.

9(Amended). [A] The method according to [any of claims 1 to 7, characterized in that] claim 1, wherein a characteristic physical property of the protected-access device is used as the unique feature.

10(Amended). [A] The method according to [any of claims 1 to 9, characterized in that] claim 1, wherein the [particular] unique feature is automatically determined and entered.

11(Amended). [A] The method according to [any of claims 1 to 10, characterized in that] claim 1, wherein the output of the PIN code is made available only for a limited time period.

12(Amended). [A] The method according to [any of claims 1 to 11, characterized in that] claim 1, wherein the protected-access devices [are] comprise smart cards and/or magnetic stripe cards.

13(Amended). [A] The method according to [any of claims 1 to 12, characterized in that] claim 1, wherein a wrong PIN code not stored is outputted if one of the two tests turns out negative.

14(Amended). An apparatus [(20)] for storing and retrieving a number of PIN codes for protected-access devices [(10)], comprising

[-] a keyboard [(26)] for entering the PIN codes and an access code,

[-] a device for receiving unique features of the protected-access devices [(10)],

[-] at least one memory for at least briefly storing the access code, storing the PIN codes and storing the unique features,

[-] a device for testing an entered access code as to its permissibility and comparing an entered unique feature with stored unique features, and

[-] a display [(25)] for indicating retrieved PIN codes.

15(Amended). [An] The apparatus according to claim 14, [characterized in that] wherein the apparatus [(20)] is a pocket card reader.

16(Amended). [An] The apparatus according to claim 13 [or 14, characterized in that] including a device for encoding the PIN codes and/or unique features and/or access code [is provided].

17(Amended). [An] The apparatus according to [any of claims 14 to 16, characterized in that] claim 14, including externally inaccessible memory areas [are provided] for storing the PIN codes and/or unique features and/or access code.

18(Amended). [An] The apparatus according to [any of claims 14 to 17, characterized in that] claim 14, wherein the keyboard [(26) forms] constitutes the device for receiving the unique features.

19(Amended). [An] The apparatus according to [any of claims 14 to 17, characterized in that] claim 14, wherein the device for receiving the unique features includes a device for automatically determining the unique features of the access-protected devices.

S:\Producer\jek\KOLBECK - KOLB3001\appendix of marked up version of claims.wpd